

SAISS

SUBCOMMITTEE ON
AUTOMATED INFORMATION
SYSTEMS SECURITY

EXECUTIVE SECRETARY

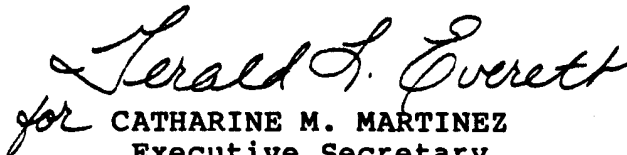
SAISS-052-85
12 September 1985

**MEMORANDUM FOR THE MEMBERS AND OBSERVERS, SUBCOMMITTEE ON
AUTOMATED INFORMATION SYSTEMS SECURITY**

SUBJECT: Minutes of the 04 September 1985 Meeting

This memorandum forwards the minutes of the 04 September 1985 meeting of the SAISS. If no written corrections or changes to these minutes are received in the Secretariat by 11 October 1985, the minutes will stand as written.

Also attached for your review are the final versions of the draft directives on Sensitive Information and AISS Education, Training and Awareness adopted at the 04 September 1985 meeting. These versions incorporate the changes agreed upon at the meeting, and reflect the editorial emendations the Secretariat was directed to make.


for CATHARINE M. MARTINEZ
Executive Secretary
Subcommittee on Automated
Information Systems Security

Encls:
a/s

Minutes of the 4 September 1985 Meeting

Subcommittee on Automated

Information Systems Security (SAISS)

I. Administrative Business

A. The Chairman convened the meeting at 1:02 pm. All members and observers were in attendance except representatives from the Office of Management and Budget, the Army, the Air Force, the Marine Corps, NASA and DUSD(P).

B. The Chairman welcomed those in attendance and referenced the corrections to the minutes of the 1 August 1985 SAISS meeting that had been submitted by the representatives from the Office of Management and Budget and the General Services Administration. No further corrections or amendments being offered, the SAISS approved the minutes as amended.

C. The Executive Secretary:

1. Announced new members and alternates in attendance;
2. Thanked the members for helping to update the membership roster;
3. Reviewed the contents of the representatives' folders, and explained how representatives could obtain a DOCKMASTER account.

II. Proposal for Definition of Sensitive, but Unclassified, National Security-Related Information

The Chairman explained the comments that had been received regarding the two alternative proposals (Alternative #1, also known as the "Burrows draft;" and Alternative #2, also known as the "Stillman draft") for the draft NTISS directive on sensitive information. The Chairman called for further comments on either draft. There being no further comments, the Subcommittee proceeded to vote. The tally was nine votes in favor of Alternative #1, and six votes in favor of Alternative #2. Following the vote adopting Alternative #1, a discussion took place about making editorial changes in the adopted draft. The discussion, initiated by Mr. Burrows, centered around polishing the wording of the Burrows draft. The Secretariat was tasked to make the required editorial changes, and to send smooth copies of the final version to SAISS representatives.

III. Proposal for AISS Education and Training and AISS Awareness

A. The SAISS Chairman recognized the Chairman of Working Group #4 (the GSA representative), who introduced the subject draft directives. The GSA representative reminded the members that Working Group #4 had been tasked at the 1 August SAISS meeting with preparing two versions of the draft directive on AISS Education and Training, both of which the membership had before them for consideration: a "stronger" version, Alternative A; and a "weaker" version, Alternative B. After a brief discussion of the costs of implementing education and training programs at various Federal agencies, the SAISS Chairman called for a vote on which alternative version to adopt. The final tally was 13 votes for Alternative A, and 3 votes for Alternative B.

B. The Subcommittee then moved to consideration of the draft directive on AISS Awareness, and adopted it by a vote of 17 to 0.

C. Following the vote on the draft directives on AISS Education and Training and AISS Awareness, the GSA representative put forward two motions: one to combine into one directive the two directives that had just been adopted; and another to add appropriate wording that would bring telecommunications within the ambit of the combined directive, and to forward that document to the STS for its consideration. The Chairman pointed out that the STS did not currently have a chairman and did not have a meeting scheduled in the near future. Several members objected to the fact that sending the directives to the STS now would just slow down the process of adoption. After a discussion of the pros and cons, the Subcommittee unanimously adopted the motion to combine the directives on AISS Education and Training and AISS Awareness into one directive, and agreed to forward the combined directive to the NTISSC. The GSA representative then withdrew his second motion.

IV. Proposal for Definition of Critical Systems

The SAISS Chairman again recognized the Chairman of Working Group #4 (the GSA representative), who introduced the subject draft directive, and pointed out the change that had been made in the latest draft version, contrasting critical systems and sensitive systems. The GSA representative also referenced comments that had been made by the OMB representative on the previous draft version to the effect that systems continuity is being addressed under a supplement to NSDD-47, and that defining critical systems is beyond the scope of NSDD-145. A discussion ensued about whether the SAISS should be addressing the criticality of systems, and it was the sense of the group that it should not. A motion was then made, duly seconded, and approved by a vote of 14 to 2, to table the issue of critical systems.

V. Proposal for Levels of Backup

The issue of critical systems having been tabled, it was suggested that there was no usefulness in discussing levels of backup for the continuity and useability of critical systems. The issue of levels of backup was then tabled by voice vote.

VI. Working Group #1 Report

The SAISS Chairman recognized the Chairman of Working Group #1 (the NSA representative), who explained that the Working Group was engaged in the process of acquiring the information necessary to draft the annual report. The NSA representative explained that the members of the Working Group had interviewed representatives from about half of the SAISS member and observer departments and agencies, and that 11 interviews remained to be conducted. He described the participants in the interviews thus far conducted as well-prepared, and urged those agencies and departments that had not yet been interviewed to avoid postponing scheduled interview sessions because it is difficult to reschedule. The Working Group #1 Chairman also encouraged members and observers not to wait if they had information to submit for the annual report, but rather to submit it now.

The SAISS Chairman reported that he had received a draft of the OMB data call figures, and surmised that there might be some slippage in the date of next year's OMB data call. The SAISS Chairman indicated that, if that were to be the case, some slippage in the date of next year's SAISS data collection effort and annual report might also be in order.

VII. NRC Comment on SAISS Membership

The Chairman recognized the observer from the Nuclear Regulatory Commission, who explained that while he was not advocating the enlargement of the SAISS, he thought other departments and agencies might have pertinent comments to make on SAISS documents that were being developed. He suggested that documents being drafted should be circulated more widely than they currently are, to such civil sector agencies as the Department of Labor, the Department of Housing and Urban Development, the Department of Health and Human Services, the Environmental Protection Agency, and the Federal Deposit Insurance Corporation, in order to obtain more well-rounded input from the federal sector.

*True to our warning about the
primary to be set up by NSDD-145
not being ideal for discussion
of sensitive IC
computer problems!*

Lin ?

The DIA representative endorsed the views of the NRC representative, pointing out that civil sector agencies need to be more aware of the problem of computer security.

Armin. The NSA representative observed that there might be a problem with getting appropriately cleared representatives from civil sector agencies that could participate in classified matters before the SAISS and its working groups.

The NCS representative noted that the documents generated by the SAISS were merely working documents, and that it should be incumbent upon the NTISSC, rather than the SAISS, to circulate documents more widely.

The representative from the Department of Transportation observed that if draft documents were distributed more widely, and the recipients of those documents had insufficient knowledge to be aware of the context in which they were drafted, the NSDD implementation process would be considerably slower.

The DCA representative concurred in the opinion expressed by the DOT representative, noting the length of time it takes to develop a consensus among the current group members and observers, and he suggested that other government departments and agencies might find it sufficient to be briefed quarterly on the activities of the SAISS.

The OJCS alternate representative suggested that perhaps a letter should be sent to the other government departments and agencies informing them of the functions of the group, and asking them if they would be interested in participating.

The Chairman obtained the sense of the SAISS that an "olive branch" should be offered to other departments and agencies, and he indicated that he would proceed on an informal basis to sound out other departments and agencies to gauge their interest in participating in the group's activities.

VIII. Closing Remarks

The SAISS Chairman endorsed the remarks made by the Chairman of Working Group #1 about members and observers not waiting to provide input to the annual report. The SAISS Chairman also told representatives present that if they had topics that they wish to place on the SAISS meeting agenda, to inform the Secretariat. The IC Staff representative asked that a briefing on TEMPEST be provided.

Whereupon, the meeting adjourned at 3:40 pm.

DRAFT

**EXECUTIVE AGENT FOR NATIONAL
TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY**

FOREWORD

National Security Decision Directive 145, dated 17 September 1984, explicitly states that a key national responsibility is to assure the security of telecommunications and automated information systems which process and communicate classified national security information, and other sensitive, but unclassified, government national security information, the loss of which could adversely affect the national security interest of the United States.

This directive establishes national security-related information as a category of sensitive, unclassified information that is judged to be vital to the national security interest, and that requires protection from unauthorized disclosure, alteration or destruction.

This directive applies to departments and agencies of the Government. The private sector is encouraged to apply the precepts of this directive wherever they perceive their information falls within the area of sensitive as defined herein.

Questions pertaining to this directive should be directed to the Executive Secretary of the National Telecommunications and Information Systems Security Committee (NTISSC).

FOR OFFICIAL USE ONLY

DRAFT

10 SEP 1985

DRAFT

NTISS Directive No.---

Date:

NATIONAL SECURITY SENSITIVE INFORMATION

Section I - Purpose

1. This directive establishes a definition for sensitive, unclassified, government or government-derived national security-related information requiring protection from unauthorized disclosure, alteration or destruction; this directive also assigns the responsibility to the heads of federal departments and agencies to identify their agency's data in accordance with the definitions established herein.

Section II - Applicability and Scope

2. This directive applies to government and government-derived information that is electronically stored, processed, transferred or communicated by federal departments and agencies, but does not apply to information that is classified for national security purposes under other national security directives and/or Executive Orders.

Section III - Authority

3. This directive, issued pursuant to National Security Decision Directive 145, National Policy on Telecommunications and Automated Information Systems Security, requires that systems handling sensitive, but unclassified, government or government-derived, information shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security.

Section IV - National Security Sensitive Information

4. This directive defines sensitive, unclassified national security-related information as separate and distinct from National Security Classified information; from non-national security-related sensitive information; and from public information; and establishes sensitive national security unclassified information as a category of information requiring protection.

5. The reader is referred to E.O. 12356, "National Security Information", dated 02 April 1982, for the definition of national security classified information.

FOR OFFICIAL USE ONLY

DRAFT

10 SEP 1985

6. Sensitive, Unclassified, Information:

a. OMB Circular A-71 (TM-1) (and its planned replacement) defines "sensitive data" as:

"'Sensitive data' is data which requires a degree of protection due to the risk and magnitude of loss or harm which could result from inadvertent or deliberate disclosure, alteration, or destruction of the data (e.g., personal data, proprietary data)."

The term "sensitive data" is further defined to include records about individuals requiring protection under the Privacy Act, proprietary data, and data not releasable under the Freedom of Information Act, as well as agency data that affect the agency's mission. Information, although neither sensitive nor sensitive, national security-related in isolation, can become sensitive national security-related when taken in aggregate.

b. This directive partitions the definition of sensitive into two categories: sensitive, national security related; and sensitive, non-national security related.

(1) Sensitive, national security-related information is unclassified information the unauthorized disclosure, alteration or destruction of which could adversely affect the national security interest.

(2) Sensitive, non-national security-related information is unclassified information which requires protection from unauthorized disclosure, alteration or destruction to a degree proportional to the risk or magnitude of loss or harm.

7. Public information. This category of unclassified government or government-derived information may be disclosed to the public without restriction but may require protection against erroneous manipulation or alteration.

Section V - Responsibilities

8. Agency heads are responsible for determining which of their data falls within the category of information described in paragraph 6.b.(1), supra, and shall provide annually, or as requested, to the National Telecommunications and Information Systems Security Committee (NTISSC), a list of their agency systems which electronically process, store, transfer or communicate such information.

DRAFT

**EXECUTIVE AGENT FOR NATIONAL
TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY**

FOREWORD

National Security Decision Directive 145, dated 17 September 1984, explicitly states that a key national responsibility is to assure the security of telecommunications and automated information systems which process and communicate classified national security information, and other sensitive, but unclassified, government national security information, the loss of which could adversely affect the national security interest of the United States. In order to achieve this end, it is essential to have a Federal workforce that is aware of and educated about problems of telecommunications and automated information systems security.

This directive establishes the requirement for federal departments and agencies to develop and implement Automated Information Systems Security (AISS) education and training programs and AISS awareness activities.

This directive applies to departments and agencies of the Government. The private sector is encouraged to apply the precepts of this directive as it sees fit.

Questions pertaining to this directive should be directed to the Executive Secretary of the National Telecommunications and Information Systems Security Committee (NTISSC).

**FOR OFFICIAL USE ONLY
DRAFT**

10 SEP 1985

DRAFT

NTISS Directive No.---

Date:

**AUTOMATED INFORMATION SYSTEMS SECURITY
EDUCATION, TRAINING, AND AWARENESS**

Section I - Purpose

This directive establishes the requirement for federal departments and agencies to develop and implement Automated Information Systems Security (AISS) education and training programs and AISS awareness activities.

Section II - Scope and Applicability

This directive is applicable to all federal departments and agencies, their employees, contractors, and licensees who develop, acquire, manage, and use automated information systems operated by, or on behalf of, the federal government to store, use, process, or communicate national security-related information.

Section III - Authority

This directive is issued pursuant to National Security Decision Directive (NSDD) 145, "National Policy on Telecommunications and Automated Information Systems Security," dated 17 September 1984, which provides for a comprehensive approach to automated information systems security.

Section IV - Rationale and Objectives

The recent and continuing evolution of information processing technologies has allowed the federal government to collect, process, and store unprecedented amounts of information. This heavy use of Automated Information Systems by the federal government has focused attention on the need to ensure that these valuable resources and the information they process are protected from conduct that would jeopardize both the mission of the Government and the interests of the public. Much of the information that the federal government possesses is classified, sensitive, or privacy-related and protected by statute; the responsibility for securing this information and the resources on which it is processed lies with the persons to whom the information and

FOR OFFICIAL USE ONLY

DRAFT

10 SEP 1985

resources are entrusted. The objective of this directive is to enhance those persons' awareness of the need to ensure the protection of data and resources; to enhance the public's confidence in the federal government's ability to provide this protection; and to support the protection of information resources at the national level through an education, training and awareness program to promote a uniform and consistent understanding of the principles and concepts of AISS.

Section V - Automated Information Systems Security Awareness

Automated Information Systems Security (AISS) education, training, and awareness activities are conducted for a wide spectrum of employees, from clerks to senior executives. AISS education, training and awareness activities must be tailored to meet the varying levels of knowledge, experience, and responsibilities of the employees. Nevertheless, there are certain basic messages that need to be conveyed. These are:

- A. The degree of reliance of the organization on automated information system resources;
- B. The potential consequences arising from the lack of adequate protection of automated information system resources;
- C. The commitment of the organization to protect automated information system resources; and,
- D. The means by which the employee can contribute to the protection of automated information system resources.

Every AISS education, training, and awareness program will contain two types of activities: initial orientation and reinforcement. The initial orientation should be conducted by an individual knowledgeable in AISS principles and concepts in a forum such as a briefing, seminar, or workshop. Reinforcement activities may take the form of "mass-appeal" media, such as posters, films, videotapes, or newsletters. These serve to provide continual reminders to the user of his or her individual responsibilities.

Section VI - Responsibilities

- A. The heads of federal departments and agencies shall:
 - 1. Designate a responsible individual within their organization to coordinate, develop, and implement an AISS education, training and awareness program.

DRAFT

2. Develop and implement an AISS education, training and awareness program.

3. Consistent with applicable laws and security requirements, make available to other federal departments and agencies any AISS education, training and awareness materials, resources or in-house educational activities.

B. The Director, National Computer Security Center shall:

1. Collect and maintain information on Automated Information Systems Security education, training and awareness; and, consistent with applicable laws and security requirements, provide this material to federal departments and agencies, federal contractors and licensees, and private sector concerns;

2. Ensure that appropriate education, training and awareness materials are developed on AISS policies, standards, criteria, products, and technologies that result from federal or federally-sponsored efforts;

3. Assess the needs of the federal government for education, training and awareness;

4. Cultivate a widespread understanding of computer security principles and concepts through contacts not only within the federal government, but with, state and local governments, the academic community, professional societies, and other parts of the private sector;

5. Develop and conduct, or assist other federal departments and agencies in developing and conducting AISS education, training and awareness activities.

3

FOR OFFICIAL USE ONLY

DRAFT

10 SEP 1985

REVISED GUIDELINES AND PROCEDURES FOR THE ISSUANCE
OF COMPARTMENTED CLEARANCES TO
THE LEGISLATIVE BRANCH

file 14.7

At the direction of the Director of Central Intelligence, to centralize the issuance of compartmented access approvals to the Legislative Branch, including staff employees of Congress, and employees of the General Accounting Office and the Library of Congress, thereby assuring the uniform and strict application of need-to-know and personnel security criteria, and to provide for an accurate, up to date, centralized record of holders of such approvals, the following guidelines and procedures are established effective immediately.

A. The DCI's Legislative Counsel shall serve as the Intelligence Community focal point for assuring the proper exercise of need-to-know pertaining to access by employees of the Legislative Branch to intelligence maintained and controlled within the SI, TK or BYE systems of compartmentation. The DCI's Legislative Counsel, acting on behalf of the DCI, shall oversee the processing of all such requests and shall validate the need-to-know. The DCI's Director of Security shall review such requests to assure proper uniform application of security criteria for access under the provisions of DCID 1/14.

B. All requests received by departments and agencies to grant employees of the Legislative Branch access to intelligence controlled within the SI, TK or BYE systems of compartmentation will be submitted by the recipient with its decision, to the DCI's Legislative Counsel for review and concurrence. Requests must clearly describe the nominee's need-to-know. Issues arising in regard to particular requests will be referred to the Director of Central Intelligence for resolution.

C. All requests for approvals of access to intelligence controlled within any system of compartmentation for any employees of the General Accounting Office or the Library of Congress will be submitted to the DCI's Legislative Counsel and will be personally approved by the DCI. Such requests must be at the direction of a Congressional committee and by letter from the committee chairman to the department or agency involved, fully stating the Congressional requirement.

D. Access to compartmented information will be approved only for permanent staff persons of Congressional committees designated by committee or subcommittee chairmen, and to selected Members of the Leadership staffs as designated by the President and President Pro-Tempore of the Senate, the Speaker of the House of Representatives and the Majority and Minority Leaders of both Houses respectively. Personal staff of Members of Congress shall not be granted compartmented clearances.

E. The following criteria will be used to establish need-to-know:

1. Direct involvement in authorization legislation pertaining to Intelligence Community agencies;
2. Direct involvement in appropriations legislation for Intelligence Community agencies;
3. Direct involvement in reviews authorized by law of activities of Intelligence Community agencies;
4. Direct involvement in oversight responsibilities carried out by the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence;
5. Direct involvement in other legislative matters which of necessity require direct access to compartmented intelligence.

In most cases, the need for substantive intelligence can be fulfilled without disclosing the source or method of acquisition. Therefore, every effort will be made to satisfy Congressional requirements for information by providing noncompartmented or sanitized material which does not reveal the manner of collection or acquisition. Direct access to compartmented information will not be approved unless sanitization or the provision of noncompartmented information is shown to be inadequate to meet the Congressional requirement.

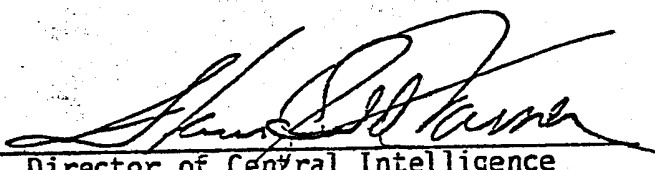
F. All requests for approvals of access to intelligence which is controlled within any system of compartmentation for any personnel designated under paragraphs C and D above must be at the direction of a committee or subcommittee Chairman and submitted by letter from that Chairman to the department or agency involved. Such a letter must include the following information:

1. Name of person requiring access
2. Date of birth
3. Social Security number
4. Position held on staff of committee or subcommittee
5. Justification for access (cite as appropriate items 1 through 5 of paragraph E above) if 5 specify nature of requirement
6. Date of last background investigation and by what department
7. Specific clearance required

G. Access approvals will be valid only so long as they are necessary, and approvals granted for particular requirements will be terminated when those requirements have been met. All approvals will be included in the central data base maintained by the Special Security Center under the direction of the DCI's Director of Security.

H. All persons, excluding Members of Congress, granted access to compartmented intelligence information shall have been the subject of a prior investigation meeting the criteria set forth in DCID 1/14. Security investigations of Congressional staff persons may be conducted under agreed upon arrangements with chairmen of committees or subcommittees, as appropriate. Investigations generally will be conducted by the Department of Defense, the FBI, or Office of Personnel Management, depending upon the particular arrangements. The agency or department sponsoring the clearance will assume responsibility for assuring the conduct of an appropriate investigation. Security determinations made by sponsoring agencies or departments will be reviewed by the DCI's Director of Security to assure the proper uniform application of security criteria under DCID 1/14.

I. No materials controlled within a system of compartmentation will be provided to any Legislative Branch requester for retention without the approval of the DCI's Legislative Counsel and unless maintained in storage facilities which meet prescribed physical security requirements and are so certified by the Special Security Center.


Director of Central Intelligence

28 June 1979

Date

All Portions of This Document
Are Unclassified